

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

## UNITED STATES DISTRICT COURT

for the  
Western District of TennesseeIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)Black Motorola Verizon cellular phone seized from  
Thomas Murray and currently in the custody of the FBI  
Memphis Child Exploitation Task Force, Memphis, TN

Case No. 20-SW-357

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A which is attached hereto and fully incorporated herein by reference

located in the Western District of Tennessee, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B which is attached hereto and fully incorporated herein by reference

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

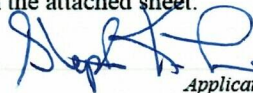
The search is related to a violation of:

Code Section	Offense Description
18 USC 2252	Possession of child pornography

The application is based on these facts:

SEE ATTACHMENT C, AFFIDAVIT OF SPECIAL AGENT STEPHEN K. LIES in support of Application for Search Warrant, which is attached hereto and fully incorporated herein by reference

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Stephen K. Lies, FBI Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
Telephone (specify reliable electronic means).

Date: 12/14/2020

City and state: Memphis, TN



Judge's signature

U.S. Magistrate Judge Charmiane G. Claxton

Printed name and title

**ATTACHMENT A**

**DESCRIPTION OF PREMISES TO BE SEARCHED:**

One Motorola Verizon cellular telephone, black in color, seized during the arrest of Thomas Murray on February 19, 2020, currently in the control and custody of the FBI Memphis Division Child Exploitation Task Force, Memphis, TN.



**ATTACHMENT B**

**Information/Items to be Seized**

**FROM WITHIN THE COLLECTED CELL PHONE AND STORAGE MEDIA**

1. For any computer, cellular phone, or storage medium whose seizure is otherwise authorized by this warrant, and any computer, cellular phone, or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
  - a. evidence that tends to identify the owner/s and user/s of said device and the files contained therein, at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;
  - d. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
  - e. evidence indicating the COMPUTER user's state of mind as it relates to the crime under investigation;
  - f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
  - g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
  - h. evidence of the times the COMPUTER was used;
  - i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;



- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
- m. contextual information necessary to understand the evidence described in this Attachment;
- n. information that can assist in the identification of any minor with whom the device was used to communicate, video chat, text, message, live stream, or speak;
- o. images of minors engaging in sexually explicit conduct or erotic conduct;
- p. communications about or with minors regarding sexual activity.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, SD Cards, USB Drives, RAM, flash memory, CD/DVD/BLU-RAY, and other magnetic or optical media.



**ATTACHMENT C**

**AFFIDAVIT OF STEPHEN K. LIES**

I, Stephen K. Lies, Special Agent of the Federal Bureau of Investigation Memphis Division, being duly sworn, state that the following information is true and correct to the best of my knowledge, information and belief:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI) and have been so employed since August 1, 1999. Since joining the FBI, I have investigated violations of federal law involving violent crimes and cybercrimes that involved the sexual exploitation of children and computer intrusions. I have been assigned full time with the Memphis Child Exploitation Task Force (MCETF) since its inception in March of 2000, the Cyber Squad of the Memphis FBI, and am currently assigned to the Civil Rights/Human Trafficking Task Force. I have gained experience through training in seminars, classes, and everyday work related to conducting these types of investigations provided by the FBI, Department of Justice and other Investigative Agencies. Just prior to joining the FBI, I was employed for approximately three years as a Computer Technician and then subsequently for three years as a Computer Network Engineer. I was also employed (prior to my FBI employment) for approximately six years as a Social Worker/Therapist who counseled children and their families involved in matters of physical and sexual abuse.



**STATUTES**

2. As an FBI Agent, your Affiant is authorized to investigate crimes involving the sexual exploitation of children pursuant to Title 18, United States Code, Section 2252(a), which makes it a federal offense to knowingly possess, access, transport, receive, or distribute a visual depiction involving the use of a minor engaging in sexually explicit conduct (as defined in 18 U.S.C. § 2256(2)(A)), if such visual depiction is of such conduct, or to attempt to do so, if that visual depiction has been mailed, shipped, or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, or the visual depiction was produced using materials that have been so mailed, shipped or transported.

3. Your Affiant has conducted and/or participated in investigations relating to the sexual exploitation of children. During these investigations I have observed and reviewed examples of child pornography in various forms of media including computer media. Your Affiant has received training and instruction in the field of investigation of child pornography, child sexual exploitation, and human trafficking and in the area of forensic extraction of digital evidence.

4. This application is part of an investigation into Thomas Murray (hereinafter Murray) and his knowing possession and distribution of visual depictions of minors engaged in sexually explicit conduct (hereinafter, "child pornography"), all in violation of Title 18 U.S.C. Section 2252(a).

5. The following information was obtained through observations and conversations of your Affiant personally, through the assistance of other law enforcement agents and agencies, including their reports, and through other sources specifically



named in this affidavit. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violation of Title 18 U.S.C. Section 2252 will be located at the premises described in **Attachment A**, and consist of or be contained in the items listed in **Attachment B**. Both attachments are incorporated by reference as if fully set forth herein.

### **PROBABLE CAUSE**

6. On or about March 3, 2019, a member of the public initiated a Cybertip to the National Center for Missing and Exploited Children (NCMEC), CyberTipline report numbered 47266419 (Incident Type: Apparent Child Pornography (Unconfirmed)) for blog content contained within the Tumblr account "underweartrucker". The content included images of a minor male posted with the following comments:

- a. (<https://undwerweartrucker.tumblr.com/post/182931161842/my-friend-johnny-has-a-cute-little-boy-this-is>) "My friend Johnny has a cute little boy. This is Him. I get to babysit while Johnny is at work and I love to watch him sleep. He wears super Mario underwear like in the picture. I like to get naked and play with them after hes (sic) worn them for a few days. They smell like his butt and that makes me even more hard."
- b. (<https://undwerweartrucker.tumblr.com/post/182929202892/i-want-him-to-ride-with-me-in-my-truck-across-the>) "I want him to ride with me in my truck across the country and never wear pants just those underwear. I'd lay him down in the back of my truck and cum all over those undies!"



7. An investigation was subsequently conducted by the FBI Memphis Crimes Against Children Task Force. Subpoena returns for the Internet Protocol (IP) addresses associated with the Tumblr “underweartrucker” account resolved to Murray, an over the road truck driver, residing in the Western District of Tennessee.

8. In April, 2019, Oath Holdings Inc (formerly Yahoo Inc) submitted two Cybertips under the incident type: Apparent Child Pornography. The two Cybertips included over 30 image files. Your Affiant reviewed these images and found some of them to depict minors engaged in sexually explicit behavior to include the lascivious exhibition of the private area and anal sex. The accounts listed in the Cybertips were “underweartrucker@yahoo” and “murraypride@yahoo”.

9. On November 5, 2019, a federal search warrant was executed on the residence of Thomas Murray. Murray was interviewed and admitted to using the aforementioned accounts to download and post sexually explicit images of minors. Murray identified the minor male and admitted to taking him on a road trip across several states in his semi-truck. During the search, one Samsung S10 cell phone was seized.

10. A review of the Samsung S10 cell phone was conducted. The phone contained images of the identified minor and sexually explicit images of Murray. The images of the minor had been altered to add text of a sexual nature. There were several email accounts set up on the phone to include “murraytrucker@yahoo”, “murraypride@gmail”, and “underwearbriefs@gmail”. The username “underweartrucker” was also found to have been used on the phone in various applications.





11. On February 19, 2020, Thomas Murray was arrested after being indicted by a Federal Grand Jury in the Western District for possession, receipt, and distribution of child pornography and for transporting a minor interstate to engage in sexual activity. At the time of his arrest one Verizon Motorola cellular telephone was seized.

12. In April 2020, your Affiant received four Cybertips initiated by the Electronic Service Providers (ESP)s Snapchat and Twitter. Twitter initiated three cybertips and Snapchat initiated one. The incident dates for the reported activity were on February 4<sup>th</sup>, 7<sup>th</sup>, and 19<sup>th</sup>, 2020, occurring after the November search warrant was executed and up to the date Murray was arrested. The Cybertips contained images, some of which depicted minors engaged in sexually explicit behavior, to include masturbation and the lascivious exhibition of the pubic area. There were also posts containing images of the identified minor who had traveled with Murray in his truck. The following account information was included in the Cybertips:

Full name: underweartrucker

Location: Memphis, TN

Additional email: [underweartrucker@gmail.com](mailto:underweartrucker@gmail.com)

Full Name: Thomas Murray

13. Your Affiant is aware that NCMEC is a private, nonprofit organization that provides services related to preventing the abduction and sexual exploitation of children. NCMEC does not conduct investigations but receives reports of child exploitation and makes those reports available to law enforcement agencies for independent review and investigation.



14. Pursuant to Title 18 U.S.C. Section 2258A, a provider of electronic communication services or remote computing services to the public through a means or facility of interstate commerce, such as the Internet, shall report incidents of apparent violations of child exploitation statutes to the CyberTipline. Such reports may include the suspect image.

#### **BACKGROUND ON CHILD EXPLOITATION MATERIAL**

15. Your Affiant, through training and experience, is aware that individuals who have an interest in possessing and sharing visual depictions of minors engaging in sexually explicit conduct ("child pornography") frequently maintain collections of images they have obtained, often for time periods of several years and longer. Digital storage options are numerous, and the storage capacity has increased, allowing for the concealment and maintenance of collections of images. Furthermore, mobile devices allow for easy access to accounts, such as email, that are stored on remote servers, making it easy for collectors to conceal their interest in child exploitation from friends, co-workers, and family members while simultaneously allowing ease of access. In addition, the declining cost of digital storage devices facilitates the maintenance of ever larger collections. Your Affiant is also aware, through training and experience, that digital storage devices have become interconnected, making it easy for even casual users of technology to transfer or copy images from one device to another, or to maintain duplicate copies on more than one device or storage medium. In fact, many devices such as smartphones can be set to automatically back up their contents to alternate storage facilities, such as laptop or desktop computers, another phone, photo-sharing websites, and cloud storage providers.

16. Your Affiant is also aware that individuals who have an interest in possessing child pornography frequently maintain collections of child erotica. These materials may, or may not, not meet the legal definition of child pornography, but, when evaluated in conjunction with other evidence, may tend to demonstrate the individual's interest in obtaining more explicit material or attempts to communicate with minors in order to obtain more explicit materials.

#### **SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS**

17. As is the case with most digital technology, communications by way of computer and cell phone can be saved or stored on the device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., in temporary files or within Internet service provider (ISP) client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

18. The search procedure for electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. on-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and



digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;

- b. on-site forensic imaging of any computers that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for examination; such imaging may require several hours to complete and require law enforcement agents to secure the search scene until that imaging can be completed;
- c. examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- d. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- e. surveying various file directories and the individual files they contain;
- f. opening files in order to determine their contents;
- g. scanning storage areas;
- h. performing key word searches through all electronic storage areas to



determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in **Attachment B**; and

- i. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in **Attachment B**.

19. Your Affiant is aware, through previous investigations, computers and cell phones are, in part or whole, manufactured outside the state of Tennessee.

20. In consideration of the foregoing, your Affiant respectfully requests that this Court issue a search warrant for the search of the Verizon Motorola cellular telephone seized during the arrest of Thomas Murray on February 19, 2020, more specifically described in **Attachment A** which is incorporated by reference as if fully set forth herein, to include any persons, vehicles, and outbuildings, authorizing the seizure and search of the items described in **Attachment B** herein.

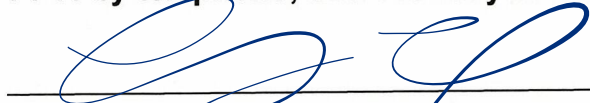
**AND FURTHER, AFFIANT SAITH NOT.**



---

**Stephen K. Lies - AFFIANT**  
**Special Agent, Federal Bureau of Investigation**

**Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 41 by telephone, this 14th day of December, 2020.**



---

**HON. CHARMIANE G. CLAXTON**  
**United States Magistrate Judge**